RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: NCS-R01

Beyond Login Attempts: Detecting Threats in SaaS Applications

Julie Agnes Sparks
Security Engineer @ Datadog

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

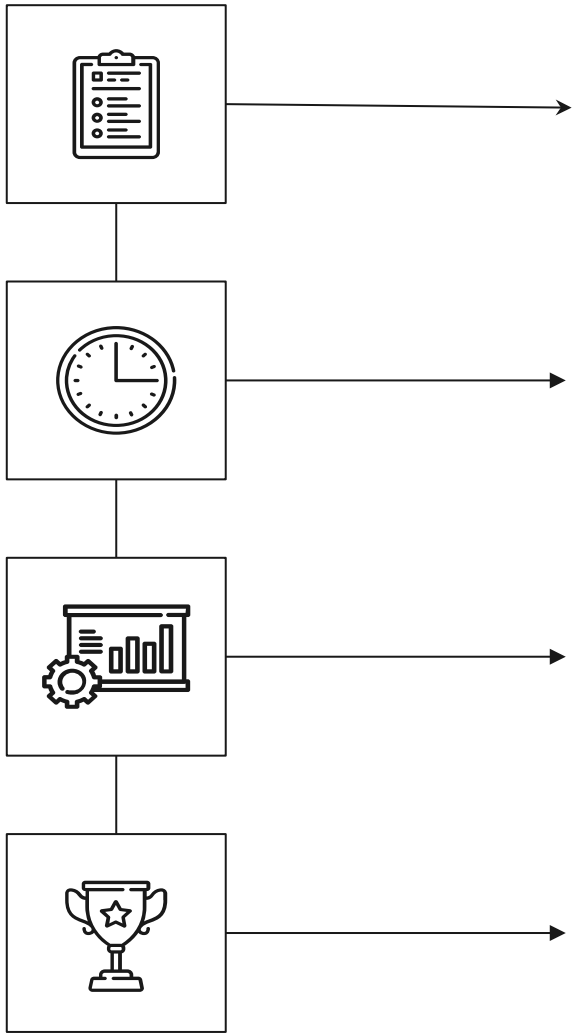
Welcome!

Currently Security Research at Datadog, formerly doing Detection & Response at Brex & Cloudflare.

Areas of expertise:

- Detection Engineering
- Incident Response
- Response Automation
- Log Ingestion
- Threat Hunting

Agenda



- Detection Engineering 101
- Logging & Data Quality
- SaaS Application Attacks
- Let’s Write Some Detections

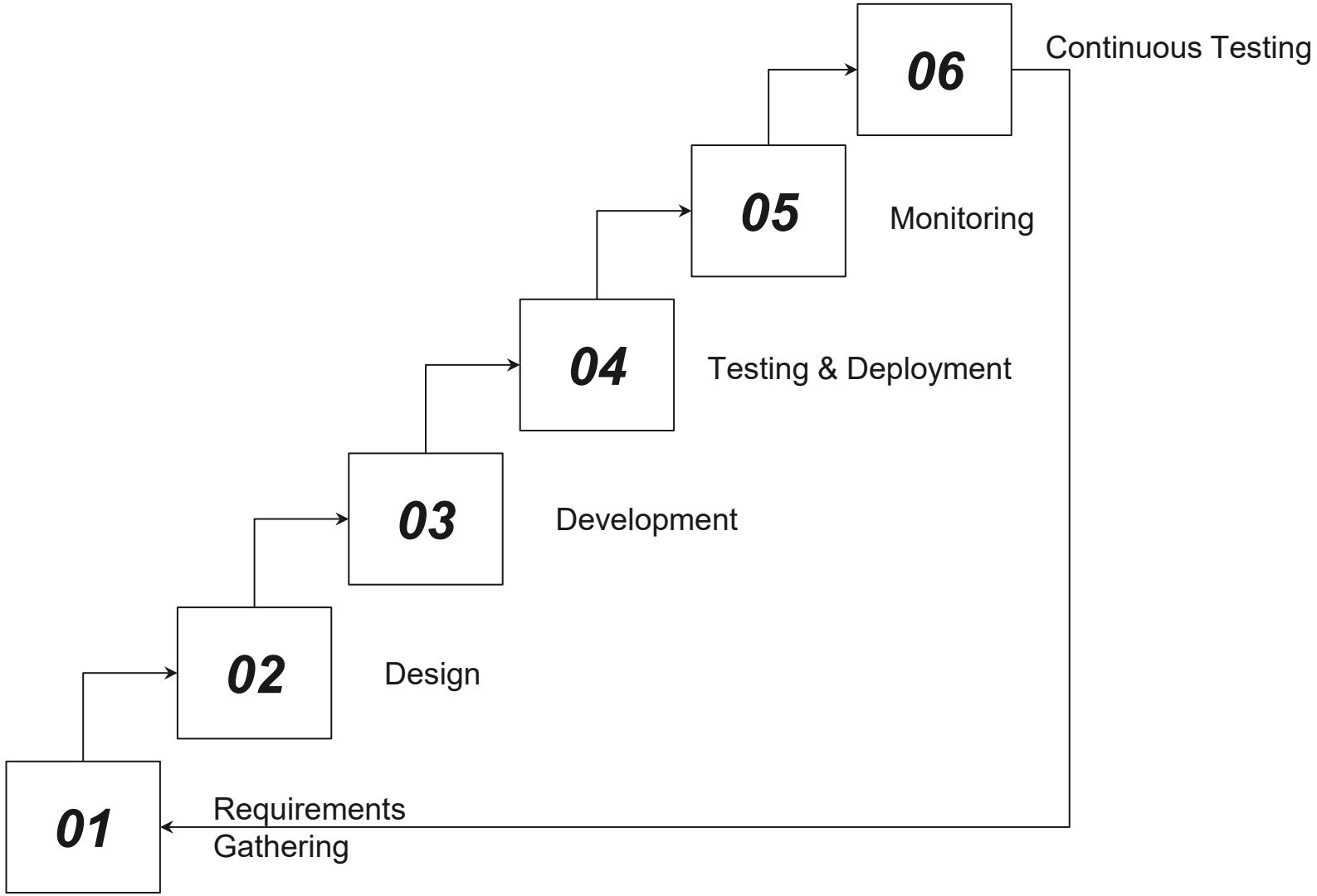
RSAC | 2025 Conference

Detection Engineering 101

What is Detection Engineering?

- Focused on detecting threats in our environments based on logs created by a system/service.
- Can be approached in a similar way to the SDLC.
- Works alongside other security functions such as incident response, cloud security, and compliance.
- Shifted to focus on detecting techniques attackers use rather than relying solely on indicators of compromise (IOCs).

Detection Development Lifecycle



DDLC

Detection as Code Principes

SDLC

Detection Development Lifecycle by Haider Dost

Detection Engineering 101

Let’s go over some key detection types…

Single Event/Streaming

Multiple Event/Batch

Risk Based

Model Based

What tools do we have for guidance?

SaaS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the SaaS platform.

View on the ATT&CK® Navigator

Version Permalink

layouts | show sub-techniques | hide sub-techniques | help

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
4 techniques	1 techniques	1 techniques	2 techniques	5 techniques	4 techniques	2 techniques	1 techniques	2 techniques
Drive-by Compromise	Valid Accounts (2)	Valid Accounts (2)	Use Alternate Authentication Material (2)	Brute Force (3)	Account Discovery (1)	Internal Spearphishing	Data from Information Repositories (1)	Endpoint Denial of Service (3)
Phishing (1)			Valid Accounts (2)	Forge Web Credentials (2)	Cloud Service Discovery	Use Alternate Authentication Material (2)		Network Denial of Service (2)
Trusted Relationship				Steal Application Access Token	Permission Groups Discovery (1)			
Valid Accounts (2)				Steal Web Session Cookie	Software Discovery (1)			
				Unsecured Credentials				

SaaS Matrix from MITRE

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
SAML enumeration	Consent phishing	Shadow workflows	API keys	Link backdooring	API keys	Password scraping
Subdomain tenant discovery	Poisoned tenants	OAuth tokens	OAuth tokens	Abuse existing OAuth integrations	OAuth tokens	API secret theft
Slug tenant enumeration	SAMLjacking	Client-side app spoofing	Evil twin integrations	Malicious mail rules	Evil twin integrations	
DNS reconnaissance	Account ambushing		Malicious mail rules		Malicious mail rules	
Username enumeration	Credential stuffing		Link sharing		Link sharing	

RSAC 2025 Conference

Logging & Data Quality

What logs can be available?

- User Activity
- API Activity
- Administrative Activity
- Integration Activity
- Authentication

User Activity Logs

- These logs capture user behavior such as access attempts, file downloads, creation of rules, and other user actions within the SaaS application.

Example: Github repository clone, Snowflake query, or Jira search.

API Activity Logs

- These logs record API calls made to the SaaS application, including the user, source IP, API endpoint accessed, and data involved.

Example: Github API request to update a repository, Gitlab deployment of project via access token.

Administrative Activity Logs

- These logs track administrative actions performed within the SaaS application, such as user creation, permission changes, or configuration modifications.

Example: Jira administrator created, Snowflake network policy for external IPs modified, etc.

Integration Activity Logs

- If your SaaS application integrates with other services, these logs track data exchange and activity related to those integrations.

Example: Snowflake client applications, Github third party application installed, etc.

Log Limitations

Lack of Log Content

Licensing & Cost

Poor Quality & Lack of Consistency in Formatting

Difficult Log Collection Mechanism

Lack of Log Content

Event types should cover all actions taken in the system and include critical fields, such as source ip address.

Audit logs should have external facing documentation on event types.

Logs should contain enough information to attribute activity to a user within the platform.

Poor Quality & Consistent Formatting

There should be log consistency across product versioning and operating systems, including when pulling the logs. Backwards compatibility introduced when needed.

There should be a low rate of log quality related incidents. Logs are reliable and can be taken as a source of truth.

There should be limited latency between when an action occurs and when the log event is available.

Difficult Log Collection Mechanisms

There should be the ability to stream logs to a cloud storage or SIEM provider (such as log push to S3).

Log collection should make it possible for event IDs to be sorted and straightforward in order to not miss log events or get duplicate events in the pipeline.

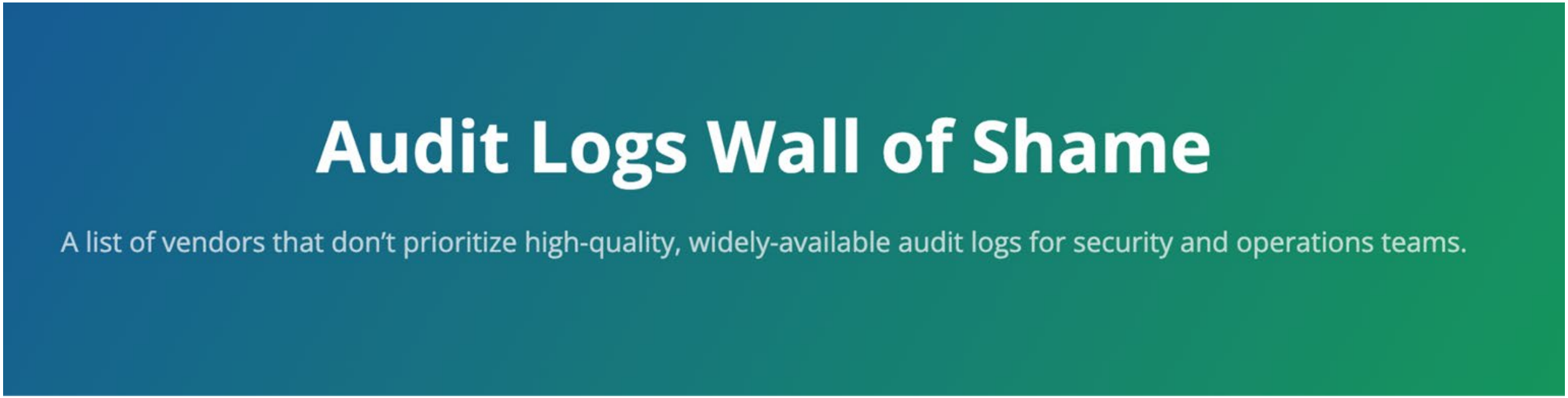
Good log formatting and data structure choice is critical, making it easy to parse logs once they are retrieved.

Licensing & Cost

There should be the ability to get detailed audit logs as part of the core product or reasonably priced.

The process to add audit logs to the contract should not be cumbersome.

Want to know more?


Audit Logs Wall of Shame
A list of vendors that don't prioritize high-quality, widely-available audit logs for security and operations teams.

Example Logging Issues for SaaS Apps

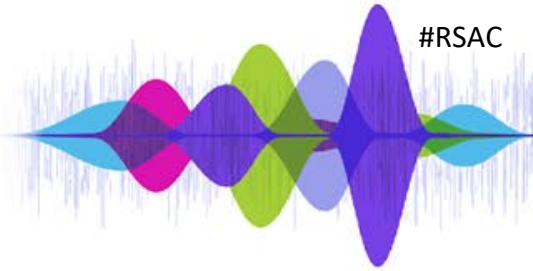
- No API collection

- Can only export logs via the UI, in batches of 500 messages per export.
- If you don't want to use the UI, you have to manually poll each machine in your environment to get the machines audit logs.

- Logs don't link to company email
- Standard logs don't include IPs
- Does not share all user activity logging with the enterprise organization
- Logged changes don't include both the new & old values

- Forces you to pay for the highest tier to stream events
- Does not include audit events for project settings, group settings, or deployment approval activity.
- The timezone used differs based on where you view audit logs (local time vs. UTC logged)

How can we make logs better ourselves?



- Reference / Lookup Tables
  - Imagine.. we had every IP address that checked in with our EDR provider in a table for device identity to reference our detections against.
    - Okta login is from a known device checked into our EDR in last 24 hours
- Data Normalization of Identities
  - Imagine… the entity field is consistent (such as user email) throughout log sources.

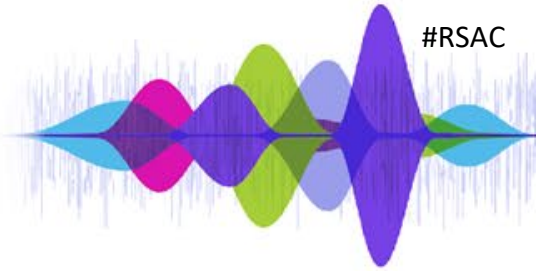
RSAC 2025 Conference

SaaS Application Attacks & Detection Opportunities

Detection Focus for SaaS

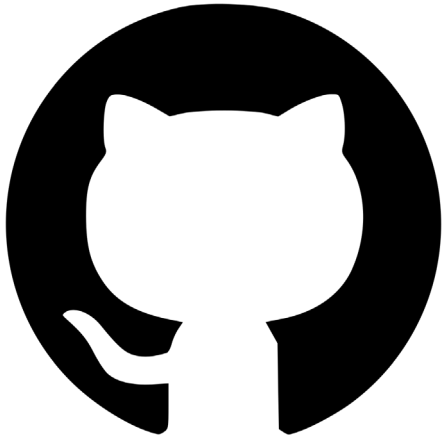
- General Areas to Consider
  - Known bad patterns (Threat Research is your best friend)
  - API activity
  - User and service account pattern analysis
  - Token usage
  - Critical assets & data access
- MITRE ATT&CK focus:
  - Initial Access
  - Persistence
  - Collection
  - Exfiltration

Inputs to Detection Engineering for SaaS



- Audit log documentation from the provider
- Past history of log data to use for hunting
- Research using current security articles and content
- Threat intelligence indicators

Let's Focus on Two Cases



Github

Developer platform for Code Interaction & Storage

Snowflake

Cloud-based data storage and analytics service

Attackers Targeting Github
Attackers Targeting Snowflake

Google Security on Github Detection
Examining Github Security
Github Security Guide

Github Log Visibility

- Github has GA attribution of associated user email addresses to activities in audit logs.
- They allow the ability to include source_ip address in logs.
- Github provides granular detail on type of token taking the action, such as:
  - Personal Access Token (Regular or Fine Grained)
  - OAuth Access Token
- There's now Github API request logs that provide granular usage of tokens to take actions via API.
- There's also some visibility into workflows that run on Github runners.

Github token formats & usage

Github Threat Actors

Various Groups

→

Malicious Payload Delivery & Compromised Packages

Github has been used to host and deliver malicious payloads and compromise dependencies used by organizations.

ShinyHunters & Various Groups

→

Credential Theft & Data Exfiltration

Compromising user accounts or applications through credential theft and then exfiltrating data, stealing further access keys, or ultimately extorting the company.

Threat Actors & Github Gitloker Extortion

Github Detection Focus

Abnormal Usage of Access Tokens

Repository Cloning Behaviors

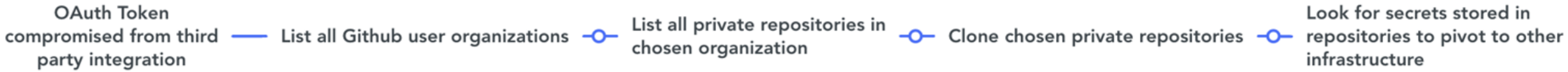
Utilizing Stolen Credentials

Persistence through New User Accounts

History of Access Token Usage

April 2022

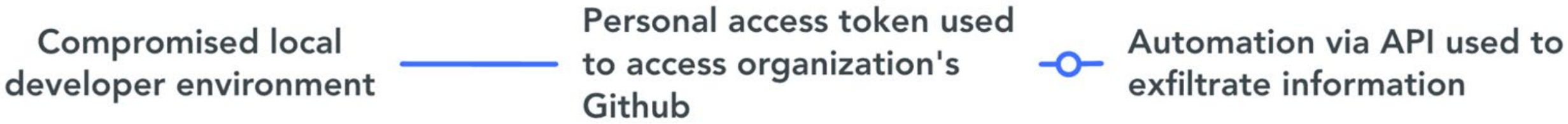
GitHub Security announced it had detected the compromise of OAuth access tokens issued to Heroku and Travis-CI integrations to download data from dozens of organizations.


OAuth Token compromised from third party integration
List all Github user organizations
List all private repositories in chosen organization
Clone chosen private repositories
Look for secrets stored in repositories to pivot to other infrastructure

History of Access Token Usage

October 2023

In another compromise, organizations found that attackers accessed their Github accounts using compromised PATs (Personal Access Token) – most likely exfiltrated silently from the victim's development environment.


Compromised local developer environment
Personal access token used to access organization's Github
Automation via API used to exfiltrate information

Github OAuth Token Actions taken by Various ASNs and UAs


```
"name": `oauth_access_asn`
"query": `source:github* @programmatic_access_type:OAuth*`
"groupByFields": `@hashed_token`
"distinctFields": `@network.client.asn`

"name": `oauth_access_ua`
"query": `source:github* @programmatic_access_type:OAuth*`
"groupByFields": `@hashed_token`
"distinctFields": `@http.useragent`

"frequency": `oauth_access_asn > 1 && oauth_access_ua > 1`
```

GitHub Personal Access Token used to clone repositories

```
"name": `personal_access_token_clones`
"query": `source:github* @evt.action:git.clone @programmatic_access_type:Personal*`
"groupByFields": `@hashed_token`
"frequency": `personal_access_token_clones > 5`
```

Github LIST Repos via API Request from OAuth or Personal Access Token

```
"name": `list_repositories_per_user_per_token"
"query": 'source:github.audit.streaming @programmatic_access_type:
(*OAuth* OR *Personal*) @evt.action:api.request @request_method:GET
@url_path:*repositories* @public_repo:False'
"groupByFields": ["@hashed_token", "@usr.name"]
```

Additional Detection Ideas

- New OAuth application authorized
- OAuth application access restrictions removed
- Private Repository changed to Public
- Anomalous service account or bot activity
- SSH key added by suspicious IP

Snowflake Threat Actors

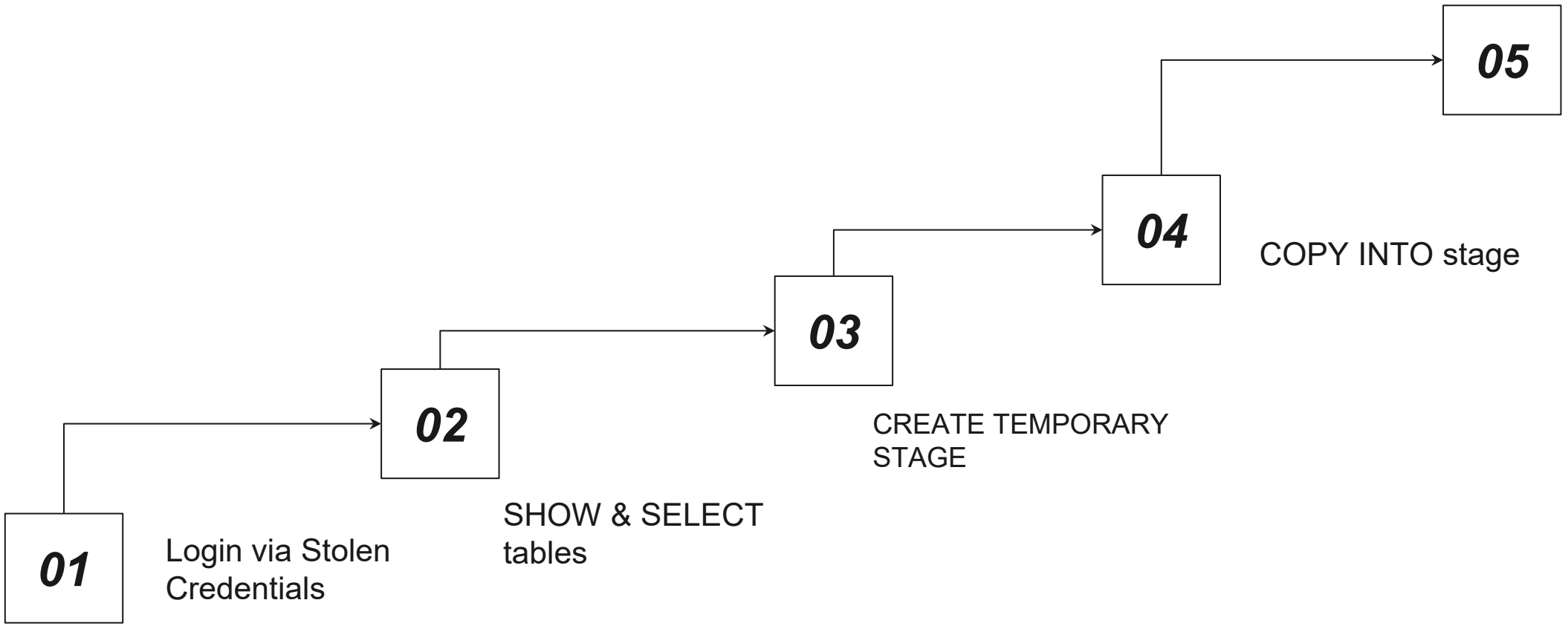
UNC 5537

Active 2024 - Present

Infostealer Malware Used to Gain User Account Access

A financially motivated threat actor suspected to have stolen a significant volume of records from Snowflake customer environments

UNC 5537 behaviors in Snowflake



Snowflake Attack Techniques

Client Applications

Exfiltration Behaviors

Malicious IP Addresses

Data Transfer Actions

Snowflake stage set to anomalous external location

```
SELECT *
FROM
  snowflake.account_usage.stages
WHERE
 NOT CONTAINS(stage_url,'companynamingconvention')
```

Snowflake user COPY INTO new location

```
SELECT *,
FROM
    snowflake.account_usage.query_history
WHERE
    CONTAINS(QUERY_TEXT, 'COPY INTO') AND CONTAINS(QUERY_TEXT, 'http')
```

Additional Detection Ideas

- New Client Application Authorized for Snowflake Instance
- Grants of Administrator role to User
- Network Policy Modified to Allow External IPs
- Anomalous amount of tables queried

Key Takeaways

- Today:
  - Learn about how you can apply SaaS threat matrices when designing new detections.
  - Gain an understanding of logging types and limitations.
- In the next two weeks:
  - Identify critical SaaS applications in your environment.
  - Implement key SaaS threat detections based on threat actor behavior across critical platforms–Github and Snowflake.

Further Resources

If you want to read more about threat hunting in Snowflake…

EMERGING THREATS AND VULNERABILITIES

A guide to threat hunting and monitoring in Snowflake

June 7, 2024

THREAT DETECTION

If you want to look at applicable detection content, check out…

- Elastic's Detection Rules repository
- Datadog's OOTB detection catalogue

RSAC 2025 Conference

Many Voices.
One Community.

Thank you!

Do you have any questions?

Reach out to me on LinkedIn or after the talk.

https://www.linkedin.com/in/julie-a-sparks/